AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

# UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
Jan. 31, 2025
CENTRAL DISTRICT OF CALIFORNIA
BY: tsn DEPUTY

United States of America
v.
Zhongliang Wang, aka "Light," and Chenyu Zhao, aka "Jimmy," aka "Xizo Yu,"

Defendants.

Case No. 2:25-mj-00437-DUTY

## CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning on or about the date of July 25, 2023, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 371 | Conspiracy |
| 18 U.S.C. § 549 | Removing Goods from Customs Custody |

This criminal complaint is based on these facts: *Please see attached affidavit.*

☒ Continued on the attached sheet.

*/s/ Martina Doino*
*Complainant's signature*

Martina Doino, Special Agent
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: January 31, 2025

*Judge's signature*

City and state: Los Angeles, California

Hon. Stephanie S. Christensen, U.S. Magistrate Judge
*Printed name and title*

AUSAs: Colin Scott 213-894-3159
Amanda Elbogen 213-894-5647

# AFFIDAVIT

I, Martina Doino, being duly sworn, declare and state as follows:

## I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since December 2019.

2. I attended the HSI Criminal Investigator Training Program at the Federal Law Enforcement Training Center ("FLETC"), in Glynco, Georgia. At FLETC, I received training in conducting criminal investigations into customs violations such as narcotics smuggling, interdiction, and distribution of controlled substances.

3. I am currently assigned to the Los Angeles Border Enforcement Security Taskforce ("LA BEST") in Los Angeles, California, and have been so assigned since August 2021. LA BEST is a multiagency task force aimed at identifying, targeting, and eliminating vulnerabilities to the security of the United States related to the Los Angeles/Long Beach seaport complex, as well as the surrounding transportation and maritime corridors. My responsibilities include the investigation of violations of federal criminal laws, including crimes involving money laundering, narcotics trafficking, smuggling, fraud, and immigration violations.

4. Prior to my tenure as a special agent, I was a police officer in Key Biscayne, Florida, from February 2015 to May

2019. From July 2018 to May 2019, I was a Task Force Officer ("TFO") on a High Intensity Drug Trafficking Area Task Force, where I participated in investigations into money laundering and drug trafficking crimes in South Florida.

## II. PURPOSE OF AFFIDAVIT

5. This affidavit is made in support of a criminal complaint and arrest warrants against Zhongliang Wang, also known as ("aka") "Light" ("**WANG**"), and Chenyu Zhao, aka "Jimmy," aka "Xiao Yu" ("**ZHAO**"), for violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody) and 18 U.S.C. § 371 (Conspiracy to Defraud the United States).

6. This affidavit is also made in support of applications for warrants to search the following:

a. The person of **WANG** as described more fully in Attachment A-1;

b. Two digital devices seized from **ZHAO** at the time of his arrest, namely, a Blue Apple iPhone 13, IMEI 351415631408650 ("SUBJECT DEVICE 1") and an Omen Transcend 14 Gaming Laptop, Serial Number 5CD415B99s, ("SUBJECT DEVICE 2," and with SUBJECT DEVICE 1, the "SUBJECT DEVICES"), as described more fully in Attachment A-2.

7. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody); 18 U.S.C. 371 (Conspiracy); 18 U.S.C. § 545 (Smuggling Goods into the United States); and 18 U.S.C. § 542 (Entry of Goods by Means of False Statements) (collectively, the "SUBJECT OFFENSES"), as

described more fully in Attachment B. Attachments A-1 and A-2, and B are incorporated herein by reference.

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrants, and search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates are approximate.

## III. Background on Cargo Container Shipments at the Port of Los Angeles

9. United States Customs and Border Protection ("CBP") is responsible for, among other things, the examination of merchandise entering the United States to ensure that it is admissible under, and in compliance with, United States laws, and the assessment and collection of taxes, fees, and duties on imported merchandise. To properly assess fees, CBP relies on a self-reporting regime in which different custom brokers inform CBP about the contents of the cargo they are trying to import into the United States.

10. Importers must supply CBP with 10 data elements when bringing goods into the United States, which includes: Seller, Buyer, Importer of Record number, Consignee number, Manufacturer/Supplier, Ship To party, Country of Origin,

Harmonized Tariff Schedule of the U.S. number (referred to as the HSTSUS number), Container Stuffing Location, and Consolidator/Stuffer Name/Address.

11. CBP has local and national targeting units that targets shipments that may yield prohibited items.

12. Once cargo has been selected for CBP examination, CBP will examine the contents of the cargo by verifying whether the manifest is accurate, whether the goods have consistent country of origin markings, whether there are contraband or smuggled goods, and inspecting for environmental, and agricultural violations, among other assessments.

13. Once the shipment has been selected for further inspection, the container is brought to a Centralized Examination Site ("CES") for further inspection. Containers are required to proceed directly to the CES after being selected for inspection.

14. The Ports of Long Beach and Los Angeles handle about 40 percent of secondary inspections for the entire country. Due to the uniquely high volume at the Port of Long Beach and Los Angeles, the transportation of the containers selected for further inspection is not always controlled by CBP. In fact, the transportation of some containers selected for inspection is controlled by the broker who filed the entry/importation paperwork. In Los Angeles, custom brokers are allowed to select their own trucking company to pick up the container and take it to a CES for further inspection. This type of drayage, which is the process by which a container is unloaded, is called broker

controlled drayage. The broker controlled drayage process is unique to the Los Angeles and Long Beach port. No other domestic ports have this policy in place.

15. Once cargo containers are ready for transportation at their place of origin, a high security bolt seal is affixed on the doors of the container, by the carrier, to maintain its integrity and to prevent any unauthorized person from gaining access to the cargo. The purpose of the high security bolt seal is to ensure that the cargo inside the container is not compromised. Each high security bolt seal has its own unique identification number that is documented on several import documents. The high security bolt seal number is assigned by the vessel carrier that will transport the sea container to its destination. Below is a picture of a high security bolt seal.

16. Title 18, United States Code Section 549 prohibits, among other things, the unauthorized and willful removal or breaking of the security seals affixed to containers while they are in customs custody and/or control.

## IV. SUMMARY OF PROBABLE CAUSE

17. **WANG**, **ZHAO**, and others, including Co-Conspirator 1, engaged in a scheme to smuggle contraband into United States through the Ports of Los Angeles and Long Beach ("Port of Los Angeles") by using fraud and deception. Specifically, **ZHAO** and Co-Conspirator 1 operated an import business out of a warehouse located on East Valley Boulevard in the City of Industry, California (the "East Valley Contraband Warehouse"), which the co-conspirators used to store smuggled contraband and otherwise coordinate their illegal import scheme.

18. On June 25, 2024, law enforcement executed a federal search warrant for the East Valley Contraband Warehouse, where agents seized significant quantities of illegal contraband, including counterfeit goods, prohibited chemicals, suspected counterfeit coins, and approximately 19.5 kilograms of enobosarm, a type of illicit steroid and Schedule V controlled substance. Agents also seized digital devices, including cellular phones belonging to **ZHAO** and Co-Conspirator 1, who were both present at the warehouse when agents executed the warrant. As detailed below, communications seized from digital devices show that **ZHAO** and Co-Conspirator 1 coordinated the diversion of shipping containers containing illegal contraband that were selected for CBP inspection so that co-conspirators could unload the contraband before presenting the container to CBP.

19. Following the search, **ZHAO**, **WANG**, and Co-Conspirator 1 continued their illegal import scheme. For example, on October

25, 2024, a cooperating source ("CS[1]") and an undercover law enforcement agent ("UC") met with **WANG** and **ZHAO** at the East Valley Contraband Warehouse to discuss the diversion of several cargo containers. Among other things, WANG and ZHAO discussed the CS transporting contraband containers in exchange for payment. The CS, working with law enforcement, delivered contraband containers to the co-conspirators in November and December of 2024 in exchange for $15,000 for each shipment.

20. On January 27, 2025, the United States Attorney's Office issued a press release announcing charges against nine defendants who allegedly engaged in an illegal smuggling scheme involving diverted cargo containers from the Port of Los Angeles. Four days later -- on January 29, 2025 -- law enforcement received an alert indicating that **ZHAO**, who is a Chinese citizen and lawful permanent resident in the United States, was scheduled to depart the United States on a one-way flight to China on January 30, 2025. On January 30, 2025, law enforcement arrested **ZHAO** at the airport before he boarded the plane. During a search incident to arrest, law enforcement seized SUBJECT DEVICE 1 from **ZHAO**'s person and SUBJECT DEVICE 2

[1] The CS's criminal history contains convictions for various misdemeanors, including driving with a suspended license, but no felonies. As discussed below, the CS was arrested and has agreed to plead guilty to conspiracy and to illegally removing goods from customs custody. The CS has agreed to cooperate with law enforcement in exchange for consideration at sentencing. The CS has provided truthful information to investigators which has been independently corroborated. On December 27, 2024, after agreeing to cooperate with government, the CS was arrested by the Ontario Police Department for possession of cocaine and carrying a loaded firearm in public. During that encounter, the CS initially told law enforcement that he did not have a firearm in his vehicle, despite having one.

from the backpack **ZHAO** was carrying. Based on the nature of **ZHAO**'s conduct and the use of digital devices used to execute the criminal scheme, there is probable cause to believe that evidence of the SUBJECT OFFENSES will be found on the SUBJECT DEVICES.

## V. STATEMENT OF PROBABLE CAUSE

21. Based on my review of law enforcement reports and other evidence, speaking with other law enforcement officers, and my personal involvement in the case, I know the following:

### A. Overview of the Illegal Smuggling Scheme

22. On February 1, 2023, CBP discovered that cargo was missing from a container that had just arrived from China, and that the missing cargo was illegally replaced, or swapped, with cargo that had clearly already entered the United States, some of which had already undergone CBP inspection.

23. This cargo swap was accomplished by using a fraudulent high security bolt seal that cloned the correctly manifested seal and its unique identification number and gave the appearance that the container had not been opened when, in fact, its contents had been removed and the fraudulent security bolt seal installed in its place.

24. HSI opened an investigation to determine how the cargo swap occurred, what cargo was removed, and who was involved in orchestrating the breaking of the seal and removal of cargo in customs custody.

25. Since then, CBP has uncovered at least 102 more incidents of "cargo swapping." That is, incidents where cargo

containers had their security seals cut and the cargo inside removed before being inspected by CBP.

26. HSI investigators have uncovered that the cargo swapping scheme is a direct result of persons illegally exploiting vulnerabilities within the customer broker drayage process at the Port of Long Beach, California.

27. As described above, CBP allows customs brokers to arrange their own transportation between the port terminals and the CES where CBP conducts inspection on imported goods that have been selected for inspection.

28. HSI has found some brokers, importers, and logistic companies are not following CBP's explicit instructions to deliver containers directly to the CES locations and are, instead, illegally diverting containers selected for CBP inspection to prevent customs inspections and bypass custom fees.

29. Specifically, instead of being brought to the CES, HSI found that some containers are brought to an offsite location, the security seal is cut, and the cargo is swapped out for recycled used items. A clone seal matching the numbers of the original seal is then placed on the container. The container is ultimately delivered to be inspected by CBP.

30. During the investigation, federal agents determined the cloned seals were being imported via international mail from China. Agents began an investigation that included intercepting air parcels, documenting the seal number, and placing CBP holds that would trigger controlled drayage on the impacted shipping

containers. This operation led to the identification of more than 40 air parcels containing approximately 88 cloned seals and 79 associated sea containers.

31. To date HSI has seized more than $1,300,000,000 worth of prohibited items that would have been diverted and entered the United States without inspection. The numbers continue to grow every day as more inspections are completed and items are discovered.

**B. Law Enforcement Identifies the East Valley Contraband Warehouse as Part of the Cargo Diversion Scheme**

32. Based on law enforcement reports that I reviewed, I know that on July 25, 2023, container number GLDU9359245 (the "245 Container") arrived in the United States at the Port of Los Angeles via the cargo vessel "Ever Leading." On July 26, 2023, CBP placed the 245 Container on hold for secondary inspection.

33. Based on its investigation, CBP suspected that the 245 Container may contain contraband. On August 18, 2023, CBP installed a global positioning system tracker ("GPS") on the 245 Container at the Arnold Peter Moller ("APM") Terminal in the Port of Los Angeles.

34. On August 24, 2023, at approximately 10:26 a.m. Pacific Standard Time ("PST"), the 245 Container was picked up by a driver working for KCS Logistics at the APM Terminal. CBP officers surveilled the container and driver, who was later identified ("Individual 2"), as he picked up the 245 Container.

35. Based on law enforcement reports, I know that law enforcement saw Individual 2 drive past the CES in Carson,

California – where the 245 Container was supposed to be inspected – and instead drive the 245 Container to the East Valley Contraband Warehouse. Based on reports from the surveilling law enforcement agents, I know the container was brought to the approximate location of the East Valley Contraband Warehouse.

36. Law enforcement agents saw that the container doors for the 245 Container were backed up against the East Valley Contraband Warehouse. Approximately 5 hours later, CBP officers observed the 245 Container arrive at the CBP Price Transfer CES at approximately 5:34 p.m. PST.

37. Upon arrival at the Price Transfer CES, HSI Task Force Officer ("TFO") Han Yit interviewed Individual 2 about the 245 Container.

38. At that time, TFO Yit inspected the bolt seal on the 245 Container and noted it appeared to be a legitimate Evergreen brand seal. However, upon closer inspection, TFO Yit saw that sections of the unique identifying number for the seal had been shaved/scraped off, and another number was laser etched over that area. TFO Yit determined the seal had been tampered with.

39. During the interview, Individual 2 stated that he owned his own truck but worked for the CS. Individual 2 told law enforcement that he gets paid approximately $150-$250 per job, depending on the destination.

40. Individual 2 stated that he picked up the 245 Container from the APM seaport terminal and was instructed by

the CS to take it to a yard in Compton prior to bringing it to the Price Transfer CES.

41. Individual 2 gave TFO Yit consent to search his cellphone. Individual 2 showed TFO Yit a text message conversation with the CS, which I have reviewed.

42. The text messages from the CS stated, "Tomorrow morning dispatch, Grab own chassis 40FT, Head to APM, Load out, GLDU9359245, Appt 0700-0800, Appt # 576443, Under KSAE, KCS logistics," and "Once you drop at Fontana Grab load from Industry valley GLDU Return to Price Transfer Tracker 25925 Under KCS logistics."

43. This string of texts shows that the CS directed Individual 2 to pick up the 245 Container from the seaport, then directed him to pick it up at a location identified as "Industry Valley," which I understand to be the East Valley Contraband Warehouse based upon where law enforcement saw the container.

### C. Law Enforcement Identifies Air Parcels Containing Fake Seals Sent to ZHAO and Co-Conspirator 1 at the East Valley Contraband Warehouse

44. On March 26, 2024, TFO Yit and I contacted CBP officers at the DHL (a global logistics and international shipping company) hub in Los Angeles, California regarding several packages that had arrived at the DHL facility from China.

45. I know from talking to other law enforcement officers that CBP conducted a border search of one of the packages after it arrived from China. Inside the package were two Matson duplicate counterfeit high security bolt seals. Matson is an

international carrier of cargo containers and has its own brand of high security bolt seals. The seal number for both bolts was 1387365. The package was labeled "hardware fittings."

46. Based on my review of a photograph of the package and discussions with other law enforcement agents, I know that the listed recipient for the package was Co-Conspirator 1, and the address on the package was the address of the East Valley Contraband Warehouse.

47. The packages were repackaged and released to be delivered. The packages were then delivered to the East Valley Contraband Warehouse.

48. The counterfeit seals inside the air parcel corresponded to a container, number MATU2576177 (the "6177 Container"), that was currently in transit from China. The 6177 Container arrived at the Port of Long Beach on March 24, 2024.

49. On April 16, 2024, CBP inspected the contents of the 6177 Container and determined it was not manifested correctly. Additionally, CBP discovered a variety of counterfeit products such as counterfeit Louis Vuitton purses, Apple products, plant items, and counterfeit pharmaceuticals.

50. After the discovery of the first air parcel on March 26, 2024, law enforcement intercepted twelve more air parcels destined for the East Valley Contraband Warehouse, which contained approximately 18 counterfeit seals. These seals corresponded to 18 cargo shipping containers destined for the Port of Long Beach, California and originating from China. Upon

discovery of the existence of the cloned seals, CBP placed inspection holds on each container.

51. Eight of these parcels were addressed to Co-Conspirator 1 at the East Valley Contraband Warehouse. Four of these parcels were addressed to Xiao Yu, which I believe to be an alias for **ZHAO** based on the fact that three of the shipments listed a phone number of ending in -5164 (the "5164 number"). The 5164 number is listed on **ZHAO**'s United States passport application as his phone number, as well on his mother's United States passport application as an emergency contact under the name **ZHAO**.

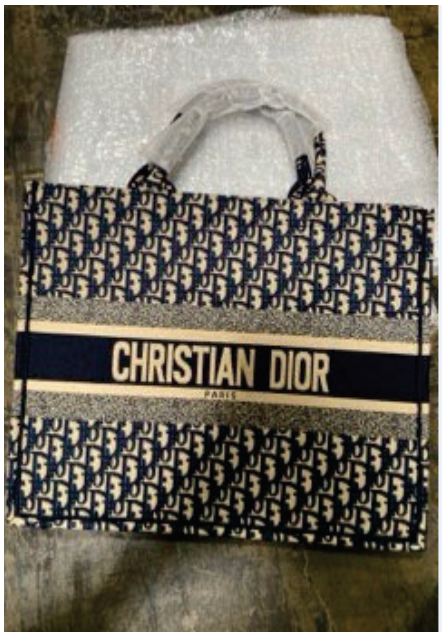
**D. Law Enforcement Searches the East Valley Contraband Warehouse and Encounters ZHAO with Significant Quantities of Counterfeit Goods**

52. On June 20, 2024, I obtained a federal search warrant signed by United States Magistrate Judge Rozella A. Oliver, in case number 24-mj-03684, to search the East Valley Contraband Warehouse.

53. I know from discussions with the law enforcement agents who executed that search warrant on June 25, 2024, that **ZHAO** was present and identified himself as the warehouse manager to the agents searching the East Valley Contraband Warehouse.

54. Inside the East Valley Contraband Warehouse, law enforcement found significant quantities of counterfeit goods, including fake luxury handbags and counterfeit shoes and sunglasses. Law enforcement also seized approximately 19.50 kilograms of a white powder, which laboratory testing later revealed to be enobosarm, or illicit steroids. The following

are photographs of some of the contraband seized from the East Valley Contraband Warehouse:


55. Based on my discussions with the law enforcement agents who executed the search warrant, I know that law enforcement seized digital devices while executing the search warrant at the East Valley Contraband Warehouse, including cellular phones belonging to **ZHAO** and Co-Conspirator 1. I have reviewed translations of messages found on Co-Conspirator 1's cellphone, which show that s/he was coordinating with contacts regarding the payment of "operating fees" for cargo containers that I know were diverted from the Port of Los Angeles. For instance, on February 5, 2024, Co-Conspirator 1 wrote to an unknown contact: "SEKU9337193 $10,000 Special handling fee issue a check To Mexican." Based on my review of law enforcement reports, I know that this refers to a container taken from the ports by the CS's company.

**E. The CS Identifies ZHAO and Co-Conspirator 1 as Part of the Cargo Diversion Conspiracy**

56. On June 29, 2024, I arrested the CS in connection with the broader cargo smuggling scheme. The CS explained to me that he worked at the direction of **ZHAO** and Co-Conspirator 1 to illegally divert cargo containers from the Port of Los Angeles and take the contraband containers to the East Valley Contraband Warehouse. Among other things, the CS explained that once the contraband containers arrived to the East Valley Contraband Warehouse, co-conspirators would unload the contraband and replace it with filler cargo. To conceal that contraband had been removed from the container, the CS also stated that co-conspirators would place a fake security seal on the container after filler materials had been placed inside. The CS also told me that he was paid up to $10,000 per container, and that he was paid in cash by Co-Conspirator 1, with **ZHAO** usually present. The CS stated he was generally paid while inside the East Valley Contraband Warehouse, during the unloading of the counterfeit cargo.

57. Based on discussions with the CS, the CS stated that he diverted cargo containers on over ten occasions to the East Valley Contraband Warehouse at the direction of **ZHAO** and Co-Conspirator 1.

58. The CS was charged federally and has agreed to plead guilty to violations of 18 U.S.C. § 371 (Conspiracy) and 18 U.S.C. § 549 (Removing Goods from Customs Custody). Due to the CS's ongoing cooperation, the indictment was filed under seal.

**F. October 25, 2024 Meeting at the East Valley Contraband Warehouse**

59. Following the execution of the federal search warrant at the East Valley Contraband Warehouse, on October 25, 2024, at approximately 2:00 p.m. PST, the UC and the CS met with **WANG** and **ZHAO** at the East Valley Contraband Warehouse to discuss a planned cargo container diversion.

60. During this meeting, which was audio recorded, **ZHAO** was introduced as "Jimmy." The parties spoke in Mandarin Chinese at the meeting. I have reviewed a summary of the event provided by the UC who attended the meeting.

61. Based on my review of the summary provided by the UC, I know the following:

a. During the meeting, the CS and **WANG** discussed an "Amazon" shipment. Based on my training and experience, and my knowledge of the investigation, I know that "Amazon" is frequently used as a code for the smuggling of products that have evaded customs. **WANG** agreed to pay the CS $15,000 to divert a cargo container with prohibited agricultural items from China.

b. During the meeting, **WANG** discussed details of the shipment and diversion, as well as his ability to handle and store refrigerated goods. **WANG** noted that he prefers to divert refrigerated cargo as the profit can be around $100,000 per container, adding that the profit for dry, non-refrigerated cargo is less than half that because demand is not as high.

c. **WANG** assured the CS that the counterfeit security seal from China would replicate and match the serial number of the security seal that would be removed from the cargo container at the time of the swapping and exchange of the contraband it contained.

d. **WANG** spoke to **ZHAO** in Mandarin Chinese about pricing for the diversion. **WANG** first indicated that he thought $8,000 would be sufficient to cover the shipment. In response, **ZHAO** shook his head to indicate that was not enough.

e. **WANG**, **ZHAO**, and the CS continued the discussion in the warehouse's business office while the UC remained by the warehouse's loading dock. The CS agreed to coordinate the movement of the cargo container from the port terminal, to remove and deliver the prohibited agricultural items to **WANG** or his agent, and to repack the container with domestic goods to provide to U.S. Customs for inspection.

f. After the meeting concluded, the CS informed the UC that the group had tentatively settled on a price of $18,000 per container swapped, and that **WANG** had expressed that he wanted the CS to conduct five container swaps per month. Based on my knowledge of the investigation, and the transaction that ultimately took place, I understand that the parties ultimately agreed on a price of $15,000 for the cargo diversion.

**G. WANG Diverts Cargo Container MAGU5749613 on November 19, 2024**

62. Based on my review of law enforcement reports, I know that on November 6, 2024, the CS received a counterfeit high-

security customs seal bearing number "R5704156" from **WANG** in the mail. My colleague, TFO Yit, looked up the seal number in law enforcement database and identified its corresponding cargo container number as MAGU5749613 ("Target Container 1").

63. Based on reporting from the CS, I understand that **WANG** had offered to pay the CS $15,000 to divert a cargo container containing prohibited agricultural items that had recently been imported to the United States from China. Specifically, **WANG** had requested that the CS coordinate the movement of the cargo container from the port terminal to an offsite location, where the CS would then transfer the prohibited agricultural items to another cargo container, then deliver that container to an address **WANG** would provide. Then, **WANG** had requested that the CS replace the contraband with "filler" cargo, drive it back to and load it onto the original cargo container, then bring that original cargo container back to the U.S. Customs CES for inspection.

64. On November 18, 2024, at **WANG**'s direction, and with the cooperation of law enforcement officers, the CS obtained an empty cargo container numbered YMLU5403975 ("Decoy Container 1").

65. On November 19, 2024, the CS, at **WANG**'s direction, coordinated the movement of Target Container 1 to another location. Unbeknownst to **WANG**, the CS worked with law enforcement to bring Target Container 1 from the port terminal to a CES location.

66. In the morning on November 20, 2024, at law enforcement's direction, CES contractors began offloading items from Target Container 1 for CBP inspection.

67. Based on CS reporting, later that morning, **WANG** provided the CS with a delivery address of a location in Monterey Park, California (the "Monterey Park location"), where WANG instructed the CS to deliver Target Container 1.

68. Based on my discussion with other law enforcement officers, I know that law enforcement then began surveillance at the Monterey Park location. Shortly after Decoy Container 1 departed the CES, surveillance agents saw a gray 2021 Toyota Sienna park in front of the garage door at the Monterey Park location. They saw an unidentified Asian male exit the Toyota Sienna and enter the Monterey Park location.

69. Surveillance agents then saw the Decoy Container arrive at the Monterey Park location.

70. Two minutes after the Decoy Container's arrival, agents saw the unidentified Asian male speaking to the driver of the Decoy Container. Shortly thereafter, the driver moved the Decoy Container down the block where he began offloading merchandise from Decoy Container 1.

71. Later that afternoon, the CS met with **WANG** at a Starbucks in Alhambra, California, where **WANG** gave the CS a blue gift bag with cash inside. The CS brought the blue gift bag to the surveilling HSI agents, who took custody of the bag, which contained $15,000 in cash.

**H. WANG Diverts Cargo Container CMAU9771359 on December 23, 2024**

72. Based on my review of law enforcement reports, I know that on December 18, 2024, the CS received a counterfeit high-security customs seal bearing number "C810955" from **WANG** in the mail. My colleague, TFO Yit, looked up the seal number in law enforcement databases and identified its corresponding cargo container number as XYLU8167921 ("Target Container 2").

73. Based on CS reporting and my review of the CS's communications, I am aware that **WANG** had again offered the CS $15,000 to divert a second cargo container also containing prohibited agricultural items that had recently been imported to the United States from China. Specifically, **WANG** again requested that the CS coordinate the movement of the cargo container from the port terminal to an offsite location, where the CS would then transfer the prohibited agricultural items to another cargo container, then deliver that container to an address **WANG** would provide. **WANG** had directed the CS to then replace the contraband with "filler" cargo, drive it back to and load it onto the original cargo container, and then bring the original cargo container back to the U.S. Customs CES for inspection.

74. On December 22, 2024, the CS directed a driver working for him to drive an empty cargo container, numbered CMAU9771359 ("Decoy Container 2"), to a CES in Los Angeles, California.

75. On December 23, 2024, the CS directed his driver to drive Target Container 2 from the port terminal to that CES.

76. In the late morning on December 23, 2024, CES contractors began offloading items from Target Container 2 for CBP inspection. At law enforcement's direction, CES contractors then transferred the uninspected items found in Target Container 2 to Decoy Container 2.

77. In the early afternoon that same day, **WANG** instructed the CS to deliver the contents of Target Container 2 to the Monterey Park location.

78. Law enforcement began surveillance at the Monterey Park location as the Decoy Container 2 departed the CES.

79. Surveillance agents later saw Decoy Container 2 arrive at the Monterey Park location.

80. Approximately one minute later, agents saw an unidentified Asian male speaking to the driver of Decoy Container 2. Shortly thereafter, the driver, who was working at the CS's direction, moved the Decoy Container down the block in Monterey Park, California, where he began offloading merchandise from Decoy Container 2.

81. Later that evening, the CS met with **WANG** at the same Starbucks as their previous meeting. **WANG** gave the CS an envelope and plastic bag that contained $15,000 in cash, which the CS gave to surveilling HSI agents, who took custody of the bag.

## I. Following the Unsealing of an Indictment Charging Nine Defendants With an Illegal Importation Scheme, ZHAO Books a One-Way Flight to China

82. As described above, on January 27, 2025, the USAO announced the unsealing of an indictment charging nine

defendants with various crimes related to an alleged illegal importation scheme. See United States v. Zheng et al., CR 24-00761-PA.

83. Two days later, on January 29, 2025, law enforcement received an alert that **ZHAO** was scheduled to depart the United States on a flight to China out of Los Angeles International Airport on January 30, 2025, at 11:50 a.m.

84. Based on my conversations with my HSI colleagues, I am aware that at approximately 12:20 p.m. PST on January 30, 2025, HSI agents approached **ZHAO** as he was boarding his flight.

85. **ZHAO** acknowledged to the agents that he was aware HSI had been to "his" warehouse referring to the East Valley Contraband Warehouse) in June 2024, and that HSI had seized his phone during the execution of the search warrant on the warehouse. **ZHAO** also acknowledged that he was aware of news coverage that had taken place earlier in the week announcing federal charges against other individuals involved in smuggling contraband through the Ports of Los Angeles and Long Beach.

86. At approximately 12:55 p.m. PST on January 30, 2025, HSI agents placed ZHAO under arrest and seized SUBJECT DEVICE 1 from **ZHAO**'s person and SUBJECT DEVICE 2 from the backpack **ZHAO** was carrying. Based on the nature of **ZHAO**'s conduct and the use of digital devices used to execute the criminal scheme, there is probable cause to believe that evidence of the SUBJECT OFFENSES will be found on the SUBJECT DEVICES.

## VI. TRAINING AND EXPERIENCE ON CUSTOM OFFENSES

87. Based on my training and experience and familiarity with custom violations investigations, I know the following:

a. Importing smuggled goods is a business that is typically lucrative and involves numerous co-conspirators, including customs brokers, delivery drivers, and warehouse workers.

b. Custom violators often maintain books, receipts, notes, ledgers, bank records, and other records relating to the importation, transportation, ordering, sale and distribution of smuggled goods at their businesses and residences and in their cars. The aforementioned records are also often maintained where the smugglers have ready access to them, such as on their cellphones, laptops, and other digital devices. Cellphones and other digital devices are often kept at businesses, residences, and cars and on the person of those engaged in this activity.

c. Communications between importers and customers buying and selling smuggled goods take place via phone calls and electronic messages, such as e-mail, text messages, and social media messaging applications, sent to and from cellphones and other digital devices. This communication includes sending photos or videos of the smuggled goods between the seller and the buyer and discussions about the negotiation of price. In addition, it is common for people engaged in customs violations to have photos and videos on their cellphones, laptops, and other digital devices of the contents of a container and the goods. Cellphones, laptops, and other digital devices are often

kept at businesses, residences, cars, and on the person of those engaged in this activity.

d. Custom violators often keep the names, addresses, and telephone numbers of their associates at their residences, businesses, and on their cellphones, laptops, and other digital devices. Violators often keep records of meetings with associates, customers, and suppliers on their cellphones, laptops, and other digital devices, including in the form of calendar entries and location data.

## VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

88. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of

evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

89. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data

in a short period of time for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

90. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition

function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress **WANG's** thumbs and/or fingers on the device(s); and (2) hold the device(s) in front of **WANG**'s face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with

certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located during the execution of the search: (1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

91. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

\\

\\

\\

## VIII. CONCLUSION

92. For all the reasons described above, there is probable cause to believe that **WANG** and **ZHAO** have committed violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody) and 18 U.S.C. § 371 (Conspiracy). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the **WANG**'s person as described more fully in Attachment A-1 as well as the SUBJECT DEVICES described in Attachment A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 31th day of January, 2025.

HONORABLE STEPHANIE CHRISTENSEN
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

PERSON TO BE SEARCHED

The person of Zhongliang Wang, aka "Light," ("WANG") (as seen in the picture below), with date of birth December 7, 1985. The search of WANG shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, folders, and bags that are within WANG's immediate vicinity and/or control at the location where the search is executed. The search shall not include a strip search or a body cavity search.

**ATTACHMENT A-2**

PROPERTY TO BE SEARCHED

The following digital devices seized during the arrest of Chenyu Zhao, aka "Jimmy," and "Xiao Yu" ("ZHAO"), which are currently held in Los Angeles, California, in the custody of Homeland Security Investigations ("HSI"):

a. A Blue Apple iPhone 13, IMEI 351415631408650 seized from ZHAO's person ("SUBJECT DEVICE 1"); and

b. An Omen Transcend 14 Gaming Laptop, Serial Number 5CD415B99s seized from ZHAO's luggage ("SUBJECT DEVICE 2").

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband fruits, or instrumentalities of violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody); 18 U.S.C. 371 (Conspiracy); 18 U.S.C. § 545 (Smuggling Goods into the United States); and 18 U.S.C. § 542 (Entry of Goods by Means of False Statements) (collectively, the "SUBJECT OFFENSES"), namely:

a. Any communications regarding the diversion of cargo containers from the Ports of Los Angeles and Long Beach;

b. Data, records, documents, programs, applications or materials relating to the smuggling of goods, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times of smuggled goods were bought, sold or otherwise distributed and any materials, documents, or records that are related to the sale, purchase, receipt, or possession of any smuggled goods, including books, receipts, photographs, bills of sale, shipping receipts, identification cards, bank statements, and correspondence discussing, requesting or confirming purchase, sale or shipment;

c. Any bills and/or subscriber documents related to digital devices used to facilitate the SUBJECT OFFENSES;

d. United States currency, money orders, or similar monetary instruments over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds);

e. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to U.S. Customs and Border Protection concerning the importation of merchandise;

f. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to logistics companies or transporters of cargo containers;

g. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to any/all customs house broker(s);

h. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

i. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any digital devices used to facilitate the SUBJECT OFFENSES and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

j. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email or social media communications or other text or written communications sent to or received from any digital device;

k. Contents of any calendar or date book, including any calendars or date books stored on any digital devices;

l. Audio recordings, photographs, video recordings or still captured images on any digital device, phone memory cards, or other storage related to the purchase, sale, transportation, or distribution of controlled substances and listed chemicals or the collection, transfer or laundering of the proceeds of illegal activities;

m. GPS coordinates and other location information or records identifying travel routes, destinations, origination points, and other locations; and

n. Any digital device used to facilitate the above listed violations and forensic copies thereof.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters,

monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

**SEARCH PROCEDURE FOR DIGITAL DEVICES**

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine

whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling

within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress **WANG**'s thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of **WANG's** face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386

(1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.